CLAIMS

1. An encryption apparatus for generating an encrypted text by encrypting a plaintext, comprising:

a storage unit operable to store an encryption key and a parameter which is adapted to a decryption apparatus and changes a probability of decryption error in decrypting the encrypted text;

an encryption unit operable to generate the encrypted text from the plaintext, using the encryption key and the parameter stored in the storage unit, according to an encryption algorithm which changes the probability of the decryption error in decrypting the encrypted text depending on a value of the parameter; and

an updating unit operable to update the parameter stored in the storage unit.

2. The encryption apparatus according to Claim 1,

wherein the updating unit updates the parameter stored in the storage unit, as time goes by.

3. The encryption apparatus according to Claim 2,

wherein the encryption unit generates the encrypted text using the encryption algorithm based on an NTRU encryption method.

4. The encryption apparatus according to Claim 3,

wherein the parameter stored in the storage unit indicates the number of terms whose coefficients indicate 1 in a random number polynomial based on the NTRU encryption method, and

the updating unit increases the number of the terms whose coefficients indicate 1, as time goes by.

5. The encryption apparatus according to Claim 4, further comprising:

an encryption key updating unit operable to receive, from the decryption apparatus, a request to update the encryption key, and update the encryption key in response to the updating request; and

an initialization unit operable to receive, from the decryption apparatus, a request to update the number of the terms whose coefficients indicate 1 in the random number polynomial, and set, in response to the updating request, the number of the terms whose coefficients indicate 1 in the random number polynomial to an initial value which decreases the probability of the decryption error to a value less than or equal to a predetermined value.

6. The encryption apparatus according to Claim 5,

wherein the initialization unit sets the number of the terms whose coefficients indicate 1 in the random number polynomial to the initial value only when the decryption apparatus has paid a predetermined amount.

7. The encryption apparatus according to Claim 2,

wherein the updating unit updates the parameter so that the probability of the decryption error in decrypting the encrypted text increases as time goes by.

8. The encryption apparatus according to Claim 1,

wherein the updating unit updates the parameter stored in the storage unit according to the number of times the encryption unit performs encryption.

9. The encryption apparatus according to Claim 8,

wherein the updating unit updates the parameter so that the probability of the decryption error in decrypting the encrypted text increases according to an increase in the number of times the

encryption apparatus performs encryption.

10. The encryption apparatus according to Claim 1,

wherein the encryption unit generates the encrypted text using an encryption algorithm based on an NTRU encryption method.

11. The encryption apparatus according to Claim 10,

wherein the parameter stored in the storage unit indicates the number of terms whose coefficients indicate 1 in a random number polynomial based on the NTRU encryption method, and

the updating unit increases the number of the terms whose coefficients indicate 1 in the random number polynomial, as time goes by.

12. The encryption apparatus according to Claim 10,

wherein the encryption unit generates the encrypted text using the encryption algorithm used for the NTRU encryption method based on an EESS (Efficient Embedded Security Standard) method.

13. The encryption apparatus according to Claim 1, further comprising:

an encryption key updating unit operable to receive, from the decryption apparatus, a request to update the encryption key, and update the encryption key in response to the updating request; and

a parameter initialization unit operable to receive, from the decryption unit, a request to update the parameter, and set, in response to the initialization request, a value of the parameter to an initial value which decreases the probability of the decryption error to a value less than or equal to a predetermined value.

14. A decryption apparatus for decrypting an encrypted text, comprising:

a decryption unit operable to generate a decrypted text using a decryption key, from the encrypted text generated according to an encryption algorithm which changes a probability of decryption error in decrypting the encrypted text depending on a value of a parameter;

a judgment unit operable to judge whether or not the decrypted text is obtained correctly;

a decryption key updating request unit operable to request an encryption apparatus to update the decryption key, according to a result of the judgment made by the judgment unit; and

a parameter initialization request unit operable to request the encryption apparatus to change the value of the parameter to an initial value which decreases the probability of the decryption error in decrypting the encrypted text to a value less than or equal to a predetermined value.

15. The decryption apparatus according to Claim 14,

wherein the decryption key updating request unit and the parameter initialization request unit send respectively, to the encryption apparatus, a request to update the decryption key and a request to initialize the parameter, together with a request to pay a predetermined amount.

16. The decryption apparatus according to Claim 15,

wherein the judgment unit judges that the decrypted text is not obtained correctly, when the probability of the decryption error in decrypting the encrypted text during a predetermined period of time exceeds a predetermined threshold.

17. The decryption apparatus according to Claim 14,

wherein the judgment unit judges that the decrypted text is not obtained correctly, when the probability of the decryption error in decrypting the encrypted text during a predetermined period of time exceeds a predetermined threshold.

18. An encryption system comprising an encryption apparatus for generating an encrypted text by encrypting a plaintext and a decryption apparatus for generating a decrypted text by decrypting the encrypted text,

wherein the encryption apparatus includes:

a storage unit operable to store an encryption key and a parameter which is adapted to the decryption apparatus and changes a probability of decryption error in decrypting the encrypted text;

an encryption unit operable to generate the encrypted text from the plaintext, using the encryption key and the parameter stored in the storage unit, according to an encryption algorithm which changes the probability of the decryption error in decrypting the encrypted text depending on a value of the parameter; and

an updating unit operable to update the parameter stored in the storage unit, and

the decryption apparatus includes:

a decryption unit operable to generate a decrypted text from the encrypted text using a decryption key;

a decryption key updating request unit operable to request the encryption apparatus to update the decryption key; and

a parameter initialization request unit operable to request the encryption apparatus to change the value of the parameter to an initial value which decreases the probability of the decryption error to a value less than or equal to a predetermined value.

19. The encryption system according to Claim 18,

wherein the updating unit updates the parameter stored in the storage unit, as time goes by.

20. The encryption system according to Claim 19,

wherein the encryption unit generates the encrypted text using an encryption algorithm based on an NTRU encryption method,

the parameter stored in the storage unit indicates the number of terms whose coefficients indicate 1 in a random number polynomial based on the NTRU encryption method, and

the updating unit increases the number of the terms whose coefficients indicate 1 in the random number polynomial, as time goes by.

21. The encryption system according to Claim 20,

wherein the decryption key updating request unit and the parameter initialization request unit respectively send, to the encryption apparatus, a request to update the decryption key and a request to initialize the parameter, together with a request to pay a predetermined amount, and

the encryption apparatus further includes:

a decryption key updating unit operable to receive, from the decryption apparatus, the request to update the decryption key, and update the decryption key in response to the updating request only when the predetermined amount is paid; and

an initialization unit operable to receive the request to initialize the parameter from the decryption apparatus, and set, in response to the initialization request, the number of the terms whose coefficients indicate 1 in the random number polynomial to an initial value which decreases a probability of decryption error to a value less than or equal to a predetermined value only when the predetermined amount is paid.

22. The encryption system according to Claim 18,

wherein the updating unit updates the parameter stored in the storage unit, according to the number of times the encryption unit performs encryption.

23. The encryption system according to Claim 18,

wherein the encryption unit generates the encrypted text using the encryption algorithm based on an NTRU encryption method.

24. The encryption system according to Claim 23,

wherein the parameter stored in the storage unit indicates the number of the terms whose coefficients indicate 1 in a random number polynomial based on the NTRU encryption method,

the decryption key updating request unit and the parameter initialization request unit respectively send, to the encryption apparatus, an instruction to update the decryption key and a request to initialize the parameter, together with a request to pay a predetermined amount, and

the encryption apparatus further includes:

a decryption key updating unit operable to receive, from the decryption apparatus, the request to update the decryption key, and update the decryption key in response to the updating request only when the predetermined amount is paid; and

an initialization unit operable to receive the request to initialize the parameter from the decryption apparatus, and set, in response to the initialization request, the number of the terms whose coefficients indicate 1 in the random number polynomial to an initial value which decreases a probability of decryption error to a value less than or equal to a predetermined value only when the predetermined amount is paid.

25. The encryption system according to Claim 18,

wherein the decryption apparatus further includes a judgment unit operable to judge whether or not the decrypted text is obtained correctly,

the decryption key updating request unit instructs the encryption apparatus to update the decryption key, according to a result of the judgment made by the judgment unit, and

the parameter initialization request unit instructs the encryption apparatus to change the value of the parameter to an initial value which decreases the probability of decryption error to a value less than or equal to a predetermined value, according to the result of the judgment made by the judgment unit.

26. An encryption method for generating an encrypted text by encrypting a plaintext, comprising:

an encrypted text generating step of generating the encrypted text from the plaintext, using an encryption key and a parameter, according to an encryption algorithm which changes a probability of decryption error in decrypting the encrypted text depending on a value of the parameter adapted to a decryption apparatus; and

an updating step of updating the parameter.

27. The encryption method according to Claim 26,

wherein in the updating step, the parameter is updated so that the probability of the decryption error in decrypting the encrypted text increases as time goes by.

28. The encryption method according to Claim 26,

wherein in the updating step, the parameter is updated so that the probability of the decryption error in decrypting the encrypted text increases according to an increase in the number of

times the encryption is performed.

29. The encryption method according to Claim 26,

wherein in the encrypted text generation step, the encrypted text is generated using the encryption algorithm based on an NTRU encryption method.

30. The encryption method according to Claim 29,

wherein the parameter indicates the number of terms whose coefficients indicate 1 in a random number polynomial based on the NTRU encryption method, and

in the updating step, the number of the terms whose coefficients indicate 1 in the random number polynomial is increased as time goes by.

31. A decryption method for decrypting an encrypted text, comprising:

a decryption step of generating a decrypted text using a decryption key, from the encrypted text generated according to an encryption algorithm which changes a probability of decryption error in decrypting the encrypted text depending on a value of a parameter;

a judgment step of judging whether or not the decrypted text is obtained correctly;

an updating request step of requesting an encryption apparatus to update the decryption key, according to a result of the judgment in the judgment step; and

an initialization request step of requesting the encryption apparatus to change the value of the parameter to an initial value which decreases the probability of decryption error to a value less than or equal to a predetermined value, according to the result of the judgment in the judgment step.

32. An encryption program for generating an encrypted text by encrypting a plaintext, causing a computer to execute the following steps of:

an encrypted text generation step of generating the encrypted text from the plaintext, using an encryption key and a parameter, according to an encryption algorithm which changes a probability of decryption error in decrypting the encrypted text depending on a value of the parameter corresponding to a decryption apparatus; and

an updating step of updating the parameter.

33. A decryption program for decrypting an encrypted text, causing a computer to execute the following steps of:

a decryption step of generating a decrypted text using a decryption key, from the encrypted text generated according to an encryption algorithm which changes a probability of decryption error in decrypting the encrypted text depending on a value of a parameter;

a judgment step of judging whether or not the decrypted text is obtained correctly;

an updating request step of requesting an encryption apparatus to update the decryption key, according to a result of the judgment in the judgment step; and

an initialization request step of requesting the encryption apparatus to change the value of the parameter to an initial value which decreases the probability of the decryption error to a value less than or equal to a predetermined value, according to the result of the judgment in the judgment step.

34. A computer-readable storage medium on which an encryption program for generating an encrypted text by encrypting a plaintext is recorded,

wherein the encryption program comprises:

an encrypted text generation step of generating the encrypted text from the plaintext, using an encryption key and a parameter, according to an encryption algorithm which changes a probability of decryption error in decrypting the encrypted text depending on a value of the parameter adapted to a decryption apparatus; and

an updating step of updating the parameter.

35. A computer-readable storage medium on which a decryption program for decrypting an encrypted text is recorded,

wherein the decryption program comprises:

a decryption step of generating a decrypted text using a decryption key, from the encrypted text generated according to an encryption algorithm which changes a probability of decryption error in decrypting the encrypted text depending on a value of a parameter;

a judgment step of judging whether or not the decrypted text is obtained correctly;

an updating request step of requesting an encryption apparatus to update the decryption key, according to a result of the judgment in the judgment step; and

an initialization request step of requesting the encryption apparatus to change the value of the parameter to an initial value which decreases the probability of the decryption error to a value less than or equal to a predetermined value, according to the result of the judgment in the judgment step.